IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A computer-readable storage medium comprising:

a first execution file recorded on said computer-readable storage medium using a copy protection mechanism, said first execution file including

authenticating means for performing an authentication process with a second execution file,

key obtaining means for obtaining unique key information unique to said first execution file, and

transmitting means for transmitting said unique key information to said second execution file,

wherein said first execution file is executed by an information processing apparatus including a processor, when said computer-readable storage medium is inserted into said information processing apparatus and said second execution file generates a content key from said unique key information, decrypts encrypted content using the content key, and reproduces the decrypted content, and

wherein said content is recorded on said computer-readable storage medium and said unique key information is used to encrypt encryption key information for encrypting digital signature information attached to said content, and said transmitting means transmits said content to said second execution file based on said digital signature information.

Claim 2 (Previously Presented): The computer-readable storage medium as claimed in claim 1, wherein said unique key information is used to encrypt encryption key information for encrypting a content.

Claim 3 (Previously Presented): The computer-readable storage medium as claimed in claim 2, wherein at least one of said second execution file and said content is recorded on said computer-readable storage medium.

Claim 4 (Cancelled).

Claim 5 (Currently Amended): An information processing apparatus into which a computer-readable storage medium is inserted, said computer-readable storage medium including a first execution file recorded using a copy protection mechanism, said information processing apparatus comprising:

a processor; and

a second execution file for reproducing an encrypted content,

wherein said second execution file includes authenticating means for performing an authentication process with said first execution file, key generating means for generating encryption key information based on unique key information obtained from said first execution file, decrypting means for decrypting said encrypted content using said encryption key information, and reproducing means for reproducing the decrypted content, and wherein said second execution file is executed when said computer-readable storage medium is inserted into the information processing apparatus, and

wherein said content is recorded on said computer-readable storage medium and said unique key information is used to encrypt encryption key information for encrypting digital signature information attached to said content, and said transmitting means transmits said content to said second execution file based on said digital signature information.

Claim 6 (Previously Presented): The information processing apparatus as claimed in claim 5, wherein said encrypted content is recorded on one of said computer-readable storage medium, in said information processing apparatus, and in a different information processing apparatus.

Claim 7 (Previously Presented): The information processing apparatus as claimed in claim 5, wherein said encrypted content is recorded on said computer-readable storage medium, said unique key information is used to encrypt encryption key information for encrypting digital signature information attached to said encrypted content, and said second execution file has receiving means for receiving said encrypted content from said first execution file based on said digital signature information.

Claim 8 (Currently Amended): An information processing method of an information processing apparatus into which a computer-readable storage medium is inserted, said computer-readable storage medium having a first execution file recorded therein using a copy protection mechanism, said information processing method comprising:

performing by a processor, an authentication process with said first execution file;

generating encryption key information based on unique key information obtained from said first execution file;

decrypting an encrypted content using said encryption key information; [[and]]

recording said content on said computer-readable storage medium;

reproducing the decrypted content;

using unique key information to encrypt encryption key information for encrypting digital signature information attached to said content; and transmitting said content to said second execution file based on said digital signature information.

Claim 9 (Previously Presented): The computer-readable storage medium as claimed in claim 2, wherein at least one of said second execution file and said content is recorded in said information processing apparatus.

Claim 10 (Previously Presented): The computer-readable storage medium as claimed in claim 2, wherein at least one of said second execution file and said content is recorded in a different information processing apparatus.